Annual Security Briefing

Purpose

- This class describes some of the basic security procedures that you should be aware of if you have been granted access to classified information. The procedures described within are not all encompassing. Only those areas that are commonly en-countered in your working environment are identified. Be sure to contact the security office for more detailed information on these and other pertinent procedures. Use this class as an introduction to security or as a security refresher/reminder.
- If you have any questions, please call us at 370-7625/7848, or email us.

Layout

- The basic information has been taken from AR 380-5 and AR 380-67. The information has been divided into sections based on functional areas performed by personnel. Within these sections, the more likely security procedures or concerns are described. If your job dictates duties other than those described, check with your security office or look at the mentioned directives for further information.

Contents

- Responsibilities
  - Managers/Supervisors
  - Individuals
  - Derog Information
- Classification Management
  - Destruction
  - Hand Carry
  - Mail
  - Reproduction
  - Fax
  - Disks
  - Preparation for movement
  - Telephone
- COMSEC

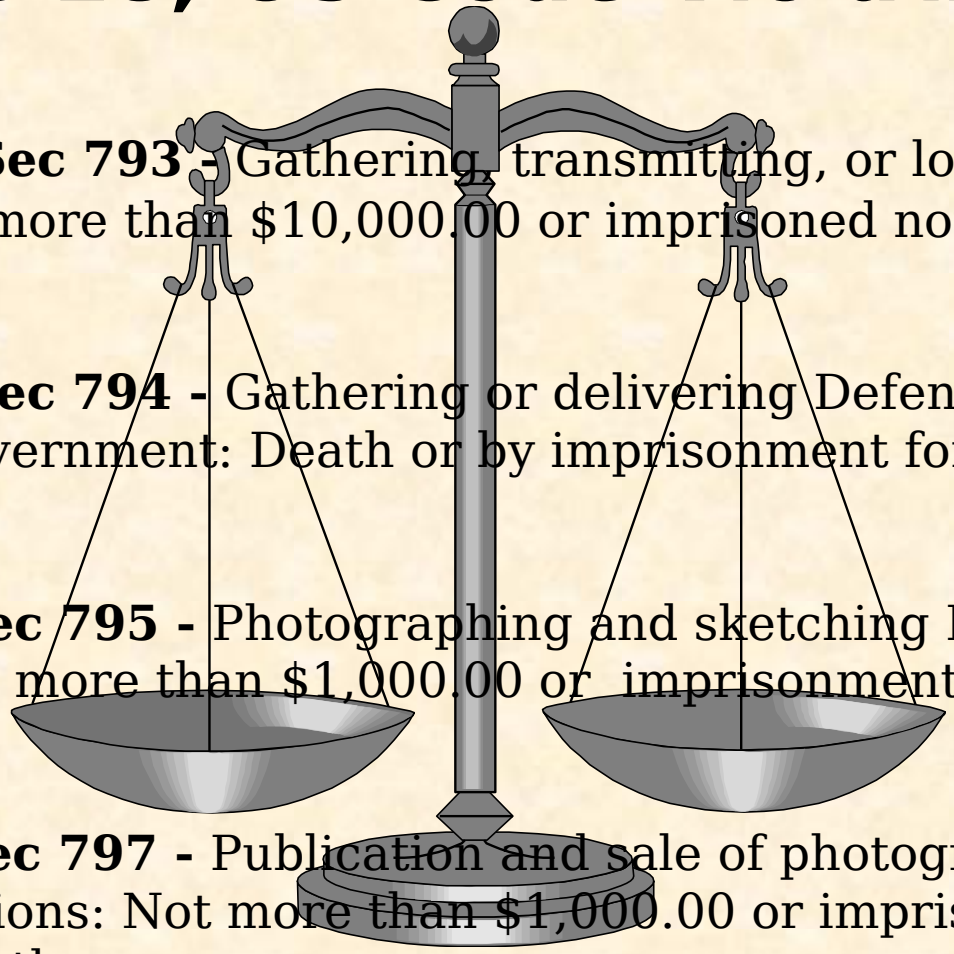
Contents (continued)

- End of the Day
- Foreign Nationals access to USAREUR Installations
- Information Systems Security and Monitoring
- OPSEC
- Personnel Security
- Physical Security
- Privately Owned Firearms
- SAEDA
- Staff Assistance Visit (SAV)

Contents (continued)

- SIGSEC
- Travel Policy
  - Reporting Foreign Travel
- Travel Warnings
  - –Consular Information Sheet
  - –Travel Advisory
  - –Public Announcements
- Where is the Threat?
- Where can I get help/assistance/answers for my questions?

Title 18, US Code Violations



- **Appendix L, Sec 793 -** Gathering, transmitting, or losing Defense information: No more than $10,000.00 or imprisoned not more that 10 years, or both.

- **Appendix M, Sec 794 -** Gathering or delivering Defense information to aid foreign government: Death or by imprisonment for any term of years, or life.

- **Appendix N, Sec 795 -** Photographing and sketching Defense installations: Not more than $1,000.00 or imprisonment not more than 1 year, or both.

- **Appendix O, Sec 797 -** Publication and sale of photographs of Defense installations: Not more than $1,000.00 or imprisoned not more than 1 year, or both.

- **Appendix P, Sec 798 -** Disclosure of classified information: Not more than $10,000.00 or imprisoned not more than 10 years, or both.

Responsibility

- Management/Supervisory
- Individuals

Managers/Supervisors Responsibility

- Ensure subordinate personnel who require access to classified information are properly cleared and are given access only to that information, to include sensitive information, for which they have a need-to-know

- Ensure subordinate personnel are trained in, understand, and follow the requirements of this regulation, and local command policy and procedures, concerning the information security program.

- Continually assess the eligibility for access to classified and sensitive information of subordinate personnel and report to the Security Manager any

Managers/Supervisors Responsibility (continued)

- Supervise personnel in the execution of procedures necessary to allow the continuous safeguarding and control of classified and sensitive information.

- Supervisors should include the protection of classified and sensitive information as a performance evaluation factor or objective for other personnel as the supervisor deems appropriate.

- Lead by example. Follow command and Army policy and procedures to properly protect classified and sensitive information and to appropriately classify and declassify information as stated in this regulation.

Individuals Responsibility

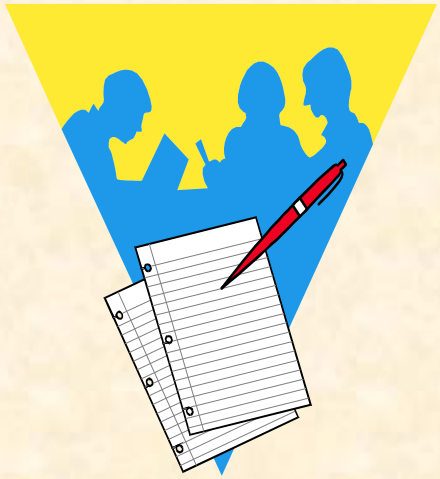
- All assigned personnel, regardless of rank, grade, title, or position, have a personal, individual, and official, responsibility to safeguard information, related to national security, that they have access to.
- All assigned personnel will report, to the proper authority, the violations by others that could lead to the unauthorized disclosure of classified and sensitive information. This responsibility CANNOT be waived, delegated, or in any other respect, excused. index

Individuals Responsibility (continued)

- All assigned personnel will safeguard all information and material, related to national security, especially classified information, which they access, and will follow the requirements of this and other applicable regulations.

Classification Management

- AR 380-5, 25 Feb 88
- Change 1, 28 Nov 89
- Change 2, 27 Jun 91
- Change 3, 17 Sep 92
- Change 4, 28 May 94
- Change 5, 21 Jul 95



index

Classified Documents

- **Individual Responsibilities**

--responsible officials will ensure that classified information is adequately protected from compromise.

- **Classification Marking**

--information or material that requires protection against unauthorized disclosure in the interest of national security shall be classified in one of three designations,namely: “Top Secret,” “Secret,” or “Confidential.”

Accountability

--any individual possessing classified material shall be responsible for providing protection and accountability for such information at al times.

- **Dissemination**

--a positive, realistic application of a “need-to-know” and security clearance in allowing access to classified information should be followed to further, not hamper, military operations

- **Discussion Involving Defense Information**

--plain and simple: “need-to-know”

- **Transmission**

--classified information may be transmitted or transported as specified in chapter VIII of AR 380-5

- **Storage**

--classified information shall be stored only under conditions adequate to prevent unauthorized persons from gaining access.

Accountability Systems

- Three book accountability, active, inactive, and destruction required for Top Secret and NATO Secret and above
- While accountability systems are not required for U.S. Secret or codeword materials, use of a DA 455 or any other simple register is recommended
- If you have any questions, comments, or concerns about this information, how it is to be stored, or how it is to be accessed, contact your security office at 370-7625/7848, or email us.

Procedures to Follow When Reproducing Classified Materials

- Use machines for which classified reproduction has been authorized and so designated
- Ensure latent images will not cause compromise
- Limitations and control procedures that apply to the originals must also be applied to the copies
- There is no authorization to copy NATO materials

▪index

Procedures to Follow When Reproducing Classified Materials, (continued)

- Always check the copier to be sure that no classified originals or copies are left in it (print three blank copies before leaving)
- Place poor copies in an authorized container and destroy them as soon as possible

Using Your Security Container

- Unless the document(s) is being accessed, it must be stored an approved, locked container.
- If leaving the office, replace the document in storage container unless someone with authorized access, and need to know, is present in the room.
- Fill out SF 702 (security container check sheet) each time you:
  - Open
  - Close, or
  - Check

  the container.

How to Mark Disks

- Use:
  - SF 706 (Top Secret label)
  - SF 707 (Secret label)
  - SF 708 (Confidential label)
  - SF 711 (data descriptor label)
  - To indicate highest level of classification contained on disk
- Place SF 710 (unclassified label) on unclassified disks that are stored with classified disks or used in an environment with classified materials
- Handle disks as if classified document ▪index

What to Do With the Disk

- Place the proper classification label on the diskette
- Store the diskette in a proper security container when:
  - You leave the area and no authorized persons are there (if there is an authorized person around, tell them that the classified diskette is there.)
  - You are not using the diskette
- Keep materials in your possession
- When returning the disc to the distribution point, ensure that it is:
  - Given to an authorized person or put it in an approved container
- Always have an individual sign for the classified document (use DA 3964)

How to Mark the Documents on Disks

- Mark portions electronically
- Apply interior page marking, overall document marking, and applicable associated marking (“derived from”, line, etc.), electronically, if feasible; otherwise mechanically (either using stamps or a typewriter) place these markings on document after it is printed
- Ensure that the electronic marking is accurate for the information provided

Minimum Marking Requirements for Paper Products

- First, mark all portions (paragraphs, drawing, caption, and subject/title lines) with highest level of classification (restrictive warning notices/caveats) found within that portion. Place marking at beginning of each portion (except subject/title lines which are marked after the portion) by using abbreviations and placing within parentheses

Minimum Marking Requirements for Paper Products

- Second, conspicuously mark at the top and bottom of each interior page (all pages except title page, if any, and first page) the highest classification of information (and restrictive caveats, if any) contained on that particular page

Minimum Marking Requirements for Paper Products

- Third, mark the top and bottom of:
  - The front cover, if any
  - The title page, if any
  - The first page, if any
  - The outside of the back cover, if any
  - With the highest level of classification of information contained within the document

Minimum Marking Requirements for Paper Products

- Fourth, for a derivatively classified document, place on the front of the document the:
  - "Derived from" line
  - "Declassify on" line
  - Downgrading instructions, if any
  - Restrictive caveats, if any
  - Originating office and date
- For clarification on the marking of original documents, please contact the security office at 370-7625/7848, or email us.

What to Do with Materials While Typing

- Do not leave the classified materials alone!!
- If you must leave:
  - Ensure that an authorized person is there (tell individual about the materials), or
  - Lock the materials in an authorized security container
  - If in an unsecured area, ensure the typewriter ribbon is secured in an appropriate security container when not being used

What to Do with the Typewriter/Printer Ribbon

- Indicate on the cartridge/cassette the classification level of the information on it. (One of the SF 706, 707, 708, 709, or 710 labels can accomplish this.) Properly destroy the cartridge/cassette as soon as feasible
- Store the cartridge/cassette in an approved security container when:
  - You leave the area and no authorized persons are there (if there is an authorized person around, be sure to tell the individual that the classified ribbon is there)
  - You are finished with your typing

What to Do with the Drafts/Notes/etc

- Store the classified drafts/notes/etc in an authorized security container
- Give it to whoever wrote it or to someone with the appropriate clearance and need-to-know
- Drafts/notes are considered to be working papers and should be marked as such. After 90 days they become permanent documents. If they are NATO or Top Secret, there is a requirement to bring them under control

Methods for Transmitting Classified Materials

- For Official Use Only:
- Information that has not been given a security classification, but which may be withheld.
- Reasons to withhold information comes under the Freedom of Information Act. (exceptions 2 thru 9)

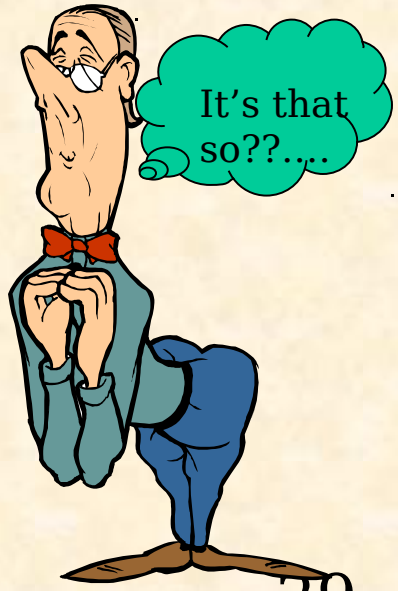
- **Release of FOUO:**
  -- Between other DoD agencies with a "Need to Know"

- **Transporting FOUO:**
  -- First class mail or parcel post

- **Telephone use:**
  -- May be discussed with other agencies

- **Disposal of FOUO:**
  --Tear or shred to preclude reconstruction

- **Markings of FOUO:**
  -- Bottom of page



Methods for Transmitting Classified Materials

- **Confidential:**
  - Authorized electronic system, e.g, a Stu-III
  - Handcarry (with proper authorization)
  - Defense Courier service (not routinely but under certain circumstances)
  - U.S. postal service registered mail to/from APO/FPO and Costa Rica
  - U.S. postal service first class mail inside the continental United States

Methods for Transmitting Classified Materials

- **Confidential, continued:**

  - Registered mail (for APO/FPO outside U.S. and Puerto Rico: for NATO outside U.S.: when uncertain if destination within U.S.: to DoD contractor or other executive branch agency, when appropriate)

  - First class mail between DoD contractor or other executive branch agency in the U.S.

  - Constant surveillance service within U.S. boundaries if item is large and bulky (Check with MTMC for information on companies that provide this service)

Methods for Transmitting Classified Materials

- **Secret:**
  - Authorization electronic system, e.g., a STU-III
  - Handcarrying (with proper authorization)
  - Defense courier service (not routinely but under certain circumstances)
  - Registered mail (within U.S. and Puerto Rico)
  - Registered mail to APO/FPO but only if mail will not pass out of U.S. control during entire mail process

Methods for Transmitting Classified Materials

- **Secret, continued:**

  - Protective security service within U.S. boundaries if item is large and bulky (check with MTMC for information on the companies that provide this service)

  - U.S. Postal service express mail (within U.S. and Puerto Rico). Do not use to send to an APO/FPO address and do not use street-side collection box.

  - GSA contract holder for overnight delivery (currently FedEx) (within US and territories). See your security office for limitations and procedures. Do not send to an APO/FPO address.

Methods for Transmitting Classified Materials

- **Top Secret:**
  - Defense courier service
  - Department of State courier service, only under rare conditions
  - Authorized electronic system, e.g. a STU-III
  - Handcarrying (with proper authorization)

Using Distribution Systems

- Ensure classified materials are not left alone in distribution boxes
- Ensure only authorized personnel (with appropriate clearance and need-to-know) pick up classified materials

Handling of Mail

- Protect mail until it has been determined whether or not classified materials are contained within
- For DoD contractors: ensure only cleared personnel receive and sign for all certified and registered mail

What to Do When No One is in the Office to Receive Mail

- Keep materials in your possession
- Take it back to the distribution point and hand it to an authorized person or put it in an approved container, or
- Deliver it to the office at a later time and hand it to an authorized person
- Always have an individual sign for the classified document (use DA 3964)

What to Do While Distributing Materials

- Keep materials in your personal possession at all times until you can hand it directly to someone else who has clearance and is authorized access to it
- Never leave classified material unattended while delivery is being made
- Ensure that it is signed for

How to Prepare Classified Materials for Movement

- Double wrap (use opaque materials)
- Place classification marking on inner layer
- Do not indicate classification on outside layer
- Seal package in such a way that tampering can be detected
- Address package to an official address, not to a person

▪index

Methods for Mailing Classified Materials

Top Secret:

- Mailing not authorized, use Defense Courier Service to transmit or
- Cleared and designated U.S. military and government civilian employees or
- If appropriate, the Department of State courier system (see AR 380-5, paragraph 8-12)

Index

Methods for Mailing Classified Documents (continued)

Secret:

- Registered mail within U.S. and Puerto Rico
- Registered mail to APO/FPO but only if mail will not pass out of U.S. control during the entire mail process
- Any means approved for transmission of Top Secret documents (see AR 380-5, paragraph 8-12)

Methods for Mailing Classified Documents, (continued)

Confidential:

- U.S. Postal service registered mail to and from APO/FPO addresses located outside the U.S. and its Territories
- Means approved for transmission of Secret material
- U.S. Postal service first class mail between DoD component locations anywhere in the U.S. and its Territories (see AR 380-5, paragraph 8-12)

Handcarrying

- Use handcarrying as your last means for transmitting classified materials. Use it only after all other transmission methods have been found inadequate
- Double wrap the materials
- Keep materials under constant surveillance and personal possession
- Do not place in detachable storage compartment, e.g. auto trailer, luggage rack, etc.
- Store overnight only at a U.S. government facility or cleared contractor facility with storage capability

▪index

Handcarrying (continued)

- Leave a list (DA 3964) of materials being handcarried with your activity
- Get briefed prior to departure
- If using a commercial airline:
  - Coordinate with the airline before leaving
  - Have ID and letter of authorization
  - Allow x-raying but do not allow direct access to the information
  - Use U.S. flag carrier or allied flag carrier if U.S. is not available
- Check with your security office for more information on handcarrying

Faxing Classified Information

- Use secure FAX unit
- Follow the encryption procedures for that piece of equipment
- Before transmitting, call the receiving office to ensure an authorized person is available to receive the transmission
- Remain with the unit until the transmission or reception is complete

▪index

Transporting from Office to Office

- Do not attract attention to yourself when carrying classified materials from one office to another. Place the materials in a nondescript envelope or container
- Place cover sheet (SF 701, 704, or 705) on materials prior to placing into envelope to remind yourself and recipient that materials are classified

Courier Orders

- Courier orders are required when you travel outside you assigned military area. The courier will be in possession of the appropriate courier authorization form as indicated below:

  - Travel within the country of assignment

  (use the DD form 2502, Courier Authorization Card)

  - Travel across international boundaries

  (use the form in AR 380-5, USAREUR Sup para 8-12 in English plus the appropriate German, Italian, Turkish or Greek, translation.)

- Travel within your city of assignment does not require courier orders, except for SCI; however, you must have permission from your supervisor to transport classified material within your area

Who Can Destroy Classified Materials

- User (or custodian) of the materials
- Designated destruction official(s) for your activity, if used
- Witness required for the destruction of Top Secret and NATO Secret information
  - Index

What to Destroy

- Check with your records management office to identify those files that are considered “record files” and “historical files” for your office
- Destroy document if it’s a “non-record” document and no operational need for it
- Conduct annual clean-out day (identify documents no longer needed and destroy); review regularly during year as well
- Recommend do a daily shred of waste

How to Destroy Classified Materials

- Burning, (if allowed by your local environmental agency)
- Shredding (particle size must meet standard set by your component)
- Pulverizing (standards for equipment set by your component)
- Pulping (standards for equipment set by your component)
- Check with your security office for location of equipment and information on other methods

Handling Classified Materials When They are Not in a Security Container

- Always ensure classified is under your direct control or that of someone who has appropriate clearance and is authorized access
- Put the appropriate clearance cover sheet (orange colored SF 703 for Top Secret; red SF 704 for Secret; blue SF 705 for Confidential) on the materials

Using Your Security Container

- Store all classified in locked container unless someone is present in the room who is authorized access
- Fill out SF 702 (security container check sheet) each time you:
  - Open
  - Close, or
  - Check the container

End of the Day Security Check

- Check the entire work area for classified materials
- Check the container to ensure it is locked
- Record this check on SF 701 (activity security checklist).
- Perform the above steps if you work with classified materials during non-working hours

Index

Who Can Have Access

- Only give access to classified material to people with appropriate clearance and a need-to-know

Discussion of Classified Information on the Phone

- Use a STU-III or some other authorized secure communication method
- Follow the encryption procedures for that piece of equipment
- Ensure that other people are not within hearing range of your voice

▪index

What Can You Do?

- Avoid sensitive topics
- Know what you will say
- Essential Elements of Friendly Information (EEFI)
- When in doubt go secure

What Else Can You Do?

- Rule 1: Avoid talking about sensitive projects and missions over unsecured communications (official DoD phone lines)
- Rule 2: Know what you are going to say before you make a telephone call or get on a radio
- Rule 3: Pay attention to your Essential Elements of Friendly Information (EEFI) and avoid talking in the unsecured mode
- Rule 4: Remember Rule 1 and use secure communications when in doubt about the sensitivity of the subject to be discussed

Where to Turn for Help?

- Assistance can be obtained from your supporting security office. They can provide a variety of services to help identify problem areas and recommend corrective actions to counter your vulnerabilities
- Call us at 370-7625/7848, or email us.

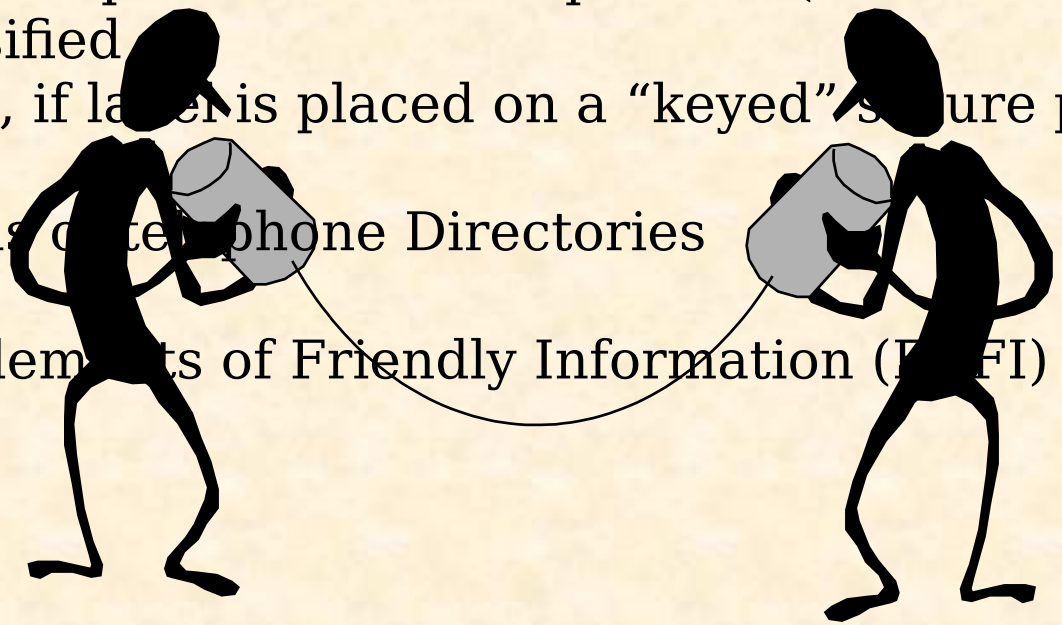
Communication Security Awareness Briefing

- Do not discuss classified information on non-secured telephones. Official DoD telephones are subject to monitoring for information systems security at all times
- DoD telephones are provided for the transmission of official government information only and are subject to information systems security monitoring at all times. Use of official DoD telephones constitutes consent to information systems security telephone monitoring in accordance with AR 380-53. All other DoD telecommunication systems are likewise provided for the transmission of official government information only and are subject to information systems security monitoring at all times. Use of official DoD telecommunications systems constitutes consent to information systems security monitoring in accordance with AR 380-53.

▪index

Transmission Security

- DD Form 2056 placed on all telephones (black out “do not discuss classified information”, if label is placed on a “keyed” secure phone)
- Destructions of telephone Directories
- Essential Elements of Friendly Information (EEFI)
- E-mail



Personnel Security

- AR 380-67, 9 Sep 88
- DA Revised PSI and Adjudicative Standards
- Individual MUST be an American Citizen

▪index

Periodic Reinvestigations

- Confidential and Secret access: NACLC, local agency checks and credit check at 10 year mark
- Top Secret access: SSBI at 5 year mark
- Go back 5 years or to the last investigation date for all required information, if the system will not validate and requests more information – provide it

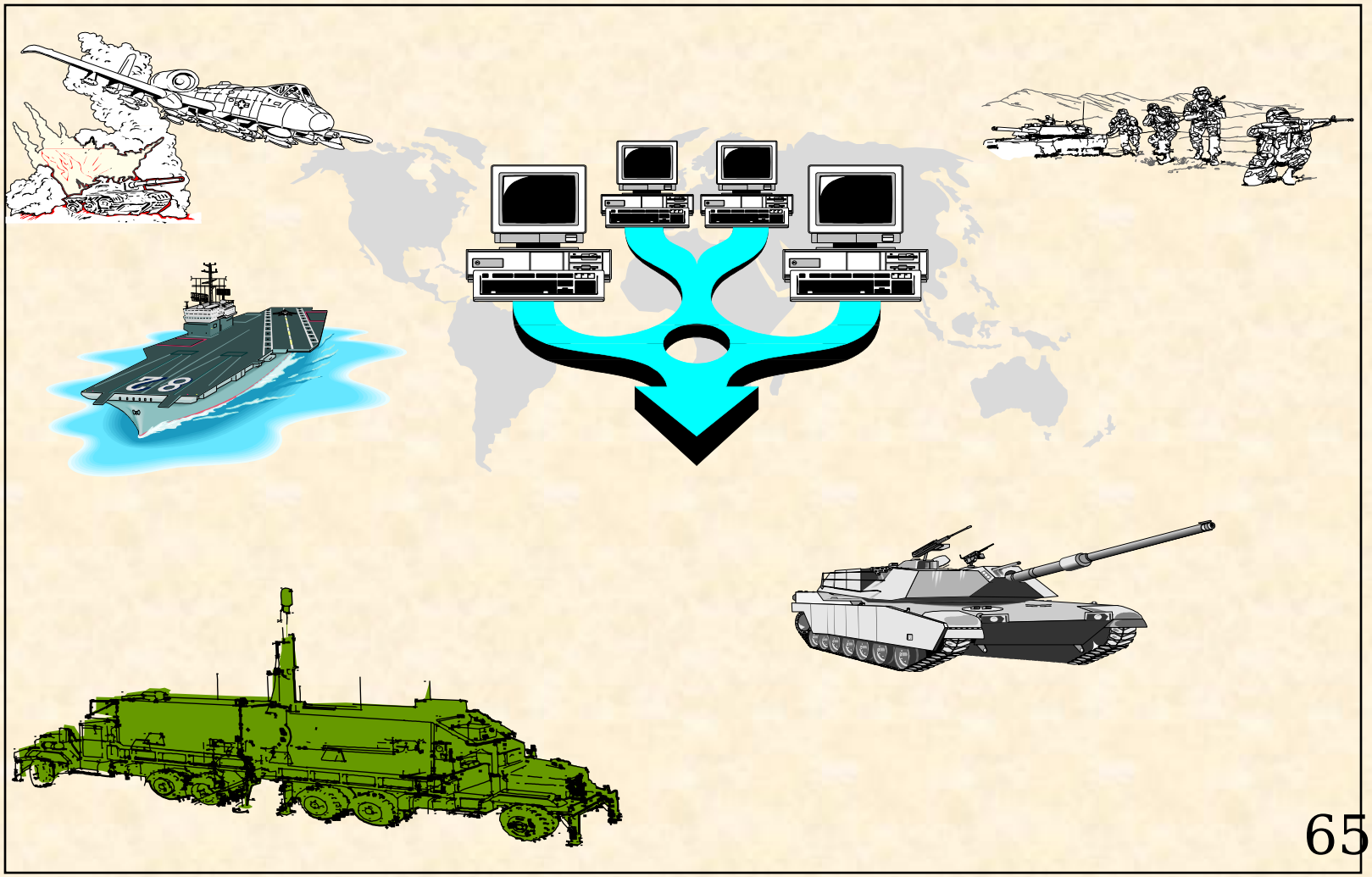
Derogatory Information

- index

Definition

- **Derogatory Information-** Any information which reflects adversely on an individual's character, honesty, loyalty, trustworthiness, financial responsibility or sense of reliability.
- IT IS EVERYONE'S RESPONSIBILITY TO REPORT DEROGATORY INFORMATION.
- If you have derogatory information, you may report it anonymously by contacting the security office at 370-7625/7848, or email us.

Information Systems Security
AR 380-19

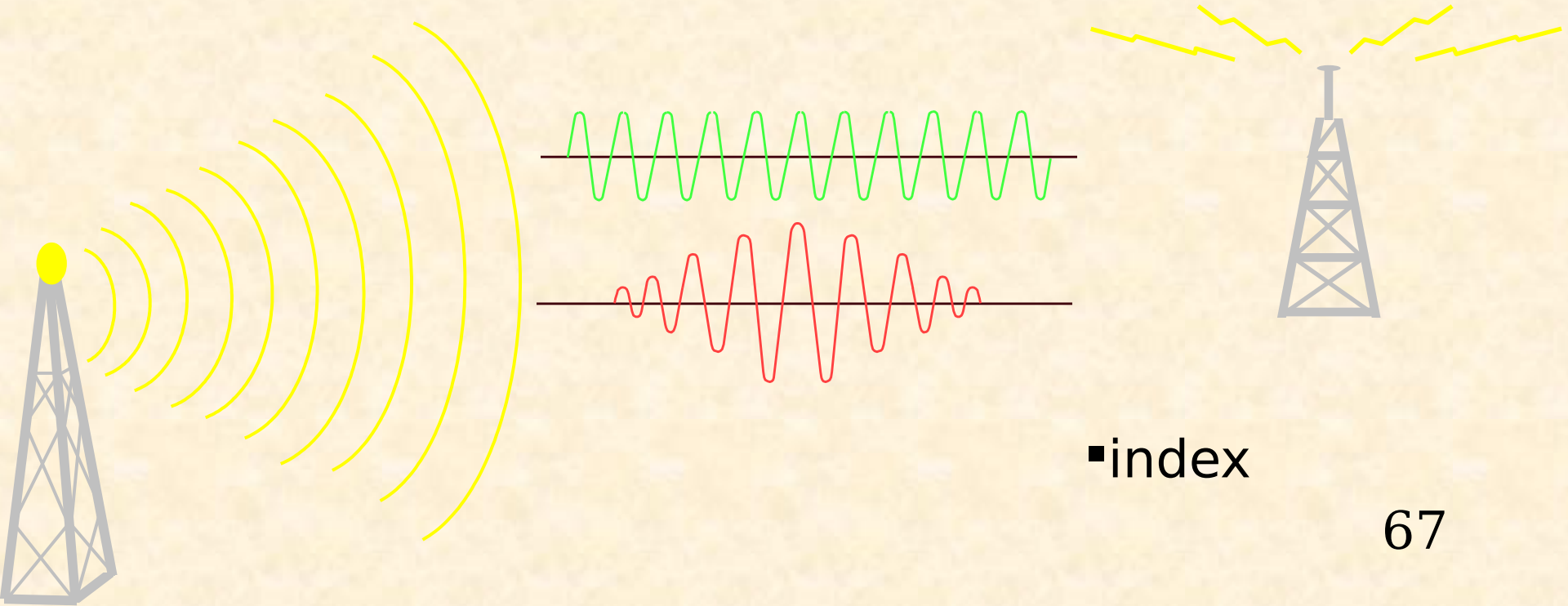


Minimum INFOSEC Requirements

- All AIS will meet and maintain the following minimum requirements in order to operate:
  - System safeguards
  - Security and training awareness
  - Software/hardware controls
  - Procedures for marking removable magnetic media
  - Marking output at the appropriate level of classification
  - Least privilege: user access only to information they need
  - Safeguards for data integrity (safeguards to detect/prevent unauthorized access and malicious codes)
  - All AIS will be accredited

Information Systems Security Monitoring

- **AR 380-53, 29 Apr 98**



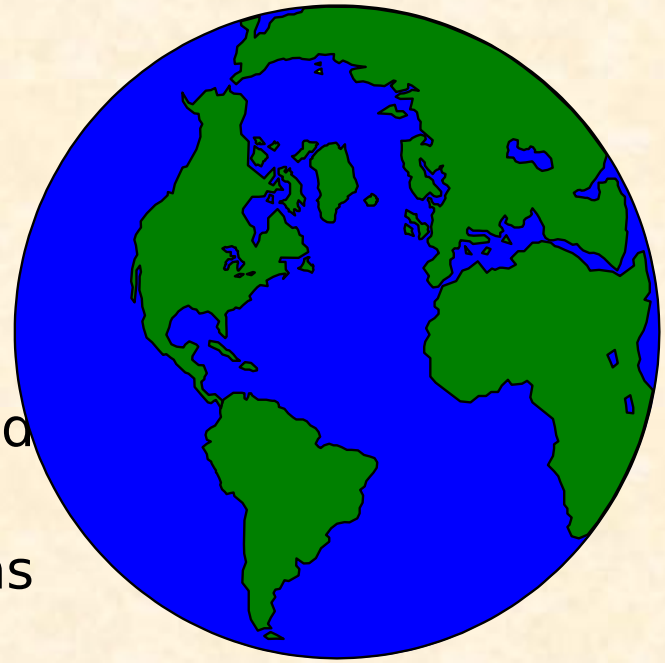
▪index

System Security Program/Safeguards

- A balanced information security program will include the following:
  - Good personnel security management/program
  - Safeguards to prevent unauthorized access to systems
    - Passwords
    - Limited access (buildings/rooms locked after duty hours, computers not left while logged on)
  - Security incident reporting procedures are established
  - Security awareness program is in place
  - ISSM/ISSO are appointed on orders and trained

AIS Threat

- 126 countries have computer espionage programs
- Reported computer break-ins are expanding at over 52%
- DoD considered “easy pickings” by computer underground
- Computer crime recognized as fastest growing component of global organized crime
- Insiders pose a major threat to systems
- Malicious codes cause loss of information and time



Types of Threats

Hackers

Insiders/Auth Users

Criminals & Organized Crime

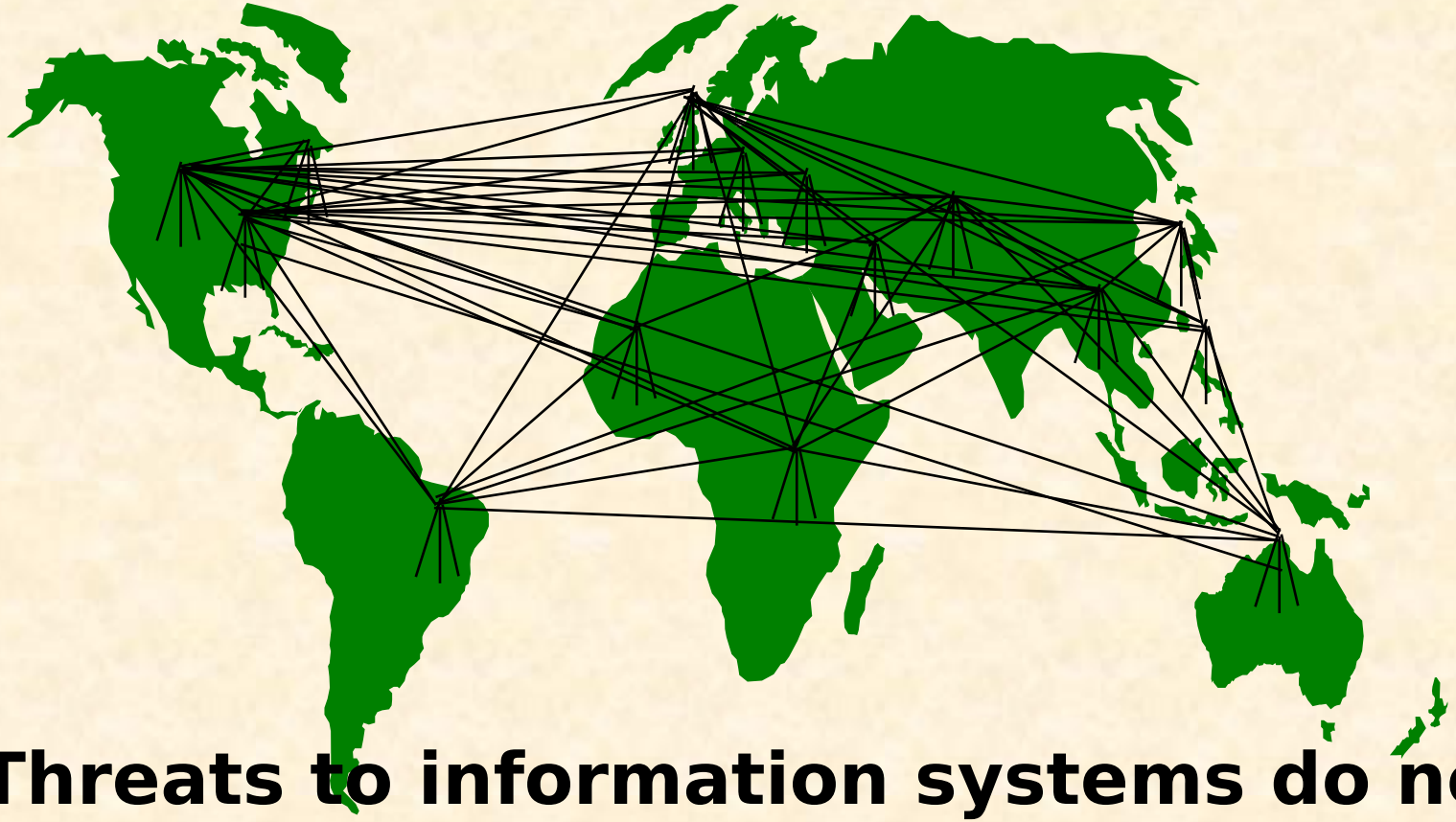
Malicious Codes

Industry & Economic Espionage

Foreign Countries

Terrorists

Information System Threat is Global



Threats to information systems do not recognize either physical or political boundaries.

Where is the Threat?

- Foreign Intelligence Services
- Industrial Espionage
- Media
- Drug Smugglers
- Criminals
- Hobbyists

index

What Type of Information Do We Disclose?

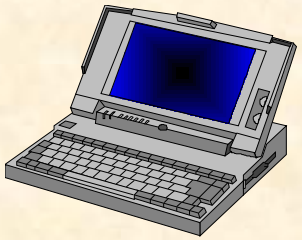
- Real work contingency operations
- Exercise information
- VIP itineraries
- Logistical information
- Communication architecture
- New systems
- Special operations

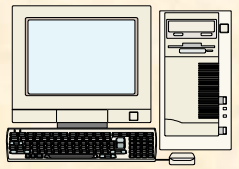
Automation Security Procedures

- All security incidents will be investigated to determine thei
- Suspected or actual incidents will be reported to your ISSC
- Preliminary inquiries will be initiated IAW AR 380-5 or AR 1

Examples of the types of incidents reportable t

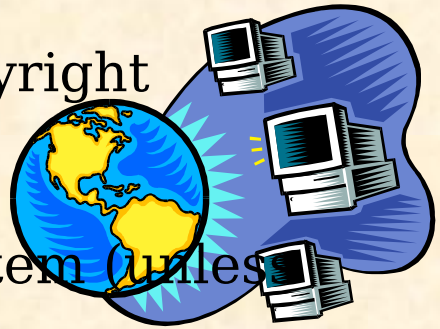
- Unexplained output at terminal
- Outputs from previous systems user remaining uncontrolled
- Unattended terminal device logged on and connected to the
- Unsuccessful log-on attempts





Automation Security Procedures

- All software will be kept locked and secured
- IM's Are responsible to ensure that copyright agreements are not being violated
- Software can only be loaded on one system (unless it has a site license)
- Privately owned software should not be use on government Unless written approval has been received from the IMO.
- DoD approved Anti-Virus software will be installed on all Government systems.
- C2 (Audit Control) software will be used on identified syste



Employee Owned Software/Hardware

Employee-owned information technology (IT) (hardware and software) may be used to process Army related work at the work place provided the commander and the designated approving authority for the network agree. Prior to connecting the IT to the network, it must meet the USAREUR Computer Security Base Line and the employee owned system will be identified in the LAN certification and accreditation document (System Security Authorization Agreement (SSAA)). DAA approval shall also be included in the LAN SSAA. All Army related information remains the property of the U.S. Government and the user will agree to sign a release from liability in case of theft, damage, or malfunction. Classified information shall not be processed on a privately owned system. When the system is no longer needed at the workplace, it will be sanitized or purged with a government endorsed product.

Employee Owned Software/Hardware

Employee-owned information technology (IT) (hardware and software) may be used to process Army related work at the work place provided the commander and the designated approving authority for the network agree. Prior to connecting the IT to the network, it must meet the USAREUR Computer Security Base Line and the employee owned system will be identified in the LAN certification and accreditation document (System Security Authorization Agreement (SSAA)). DAA approval shall also be included in the LAN SSAA. All Army related information remains the property of the U.S. Government and the user will agree to sign a release from liability in case of theft, damage, or malfunction. Classified information shall not be processed on a privately owned system. When the system is no longer needed at the workplace, it will be sanitized or purged with a government endorsed product.

Automation Security Procedures

Access to microcomputers must be limited to authorized users

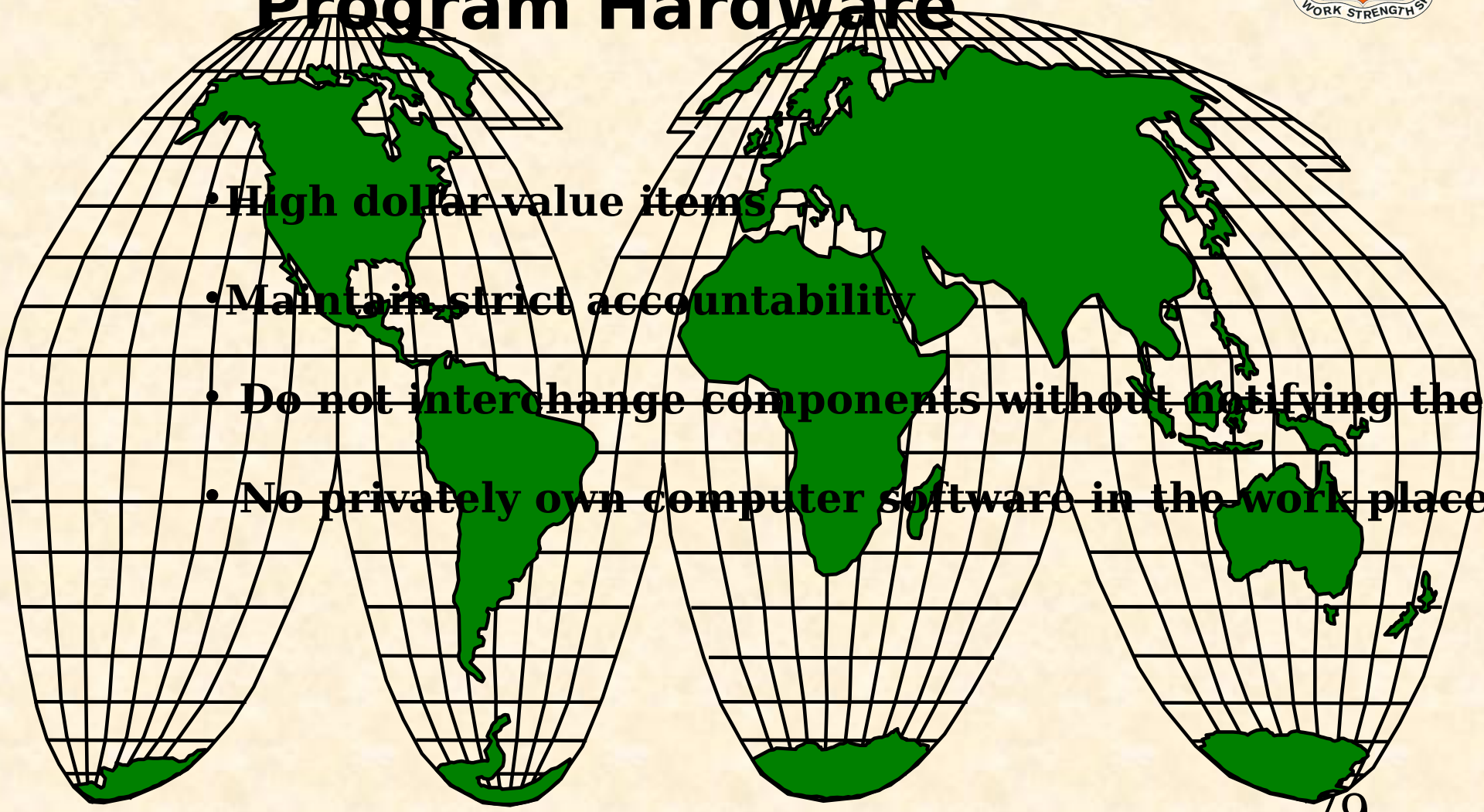
This system is a "high dollar" item. It must be afforded the ap
security measures. Locked doors during non-duty operations

Privately own computers will not be permitted in t

- **Classification Marking:**
  -- All computer equipment will be properly marked
  the highest classification processed on the syste

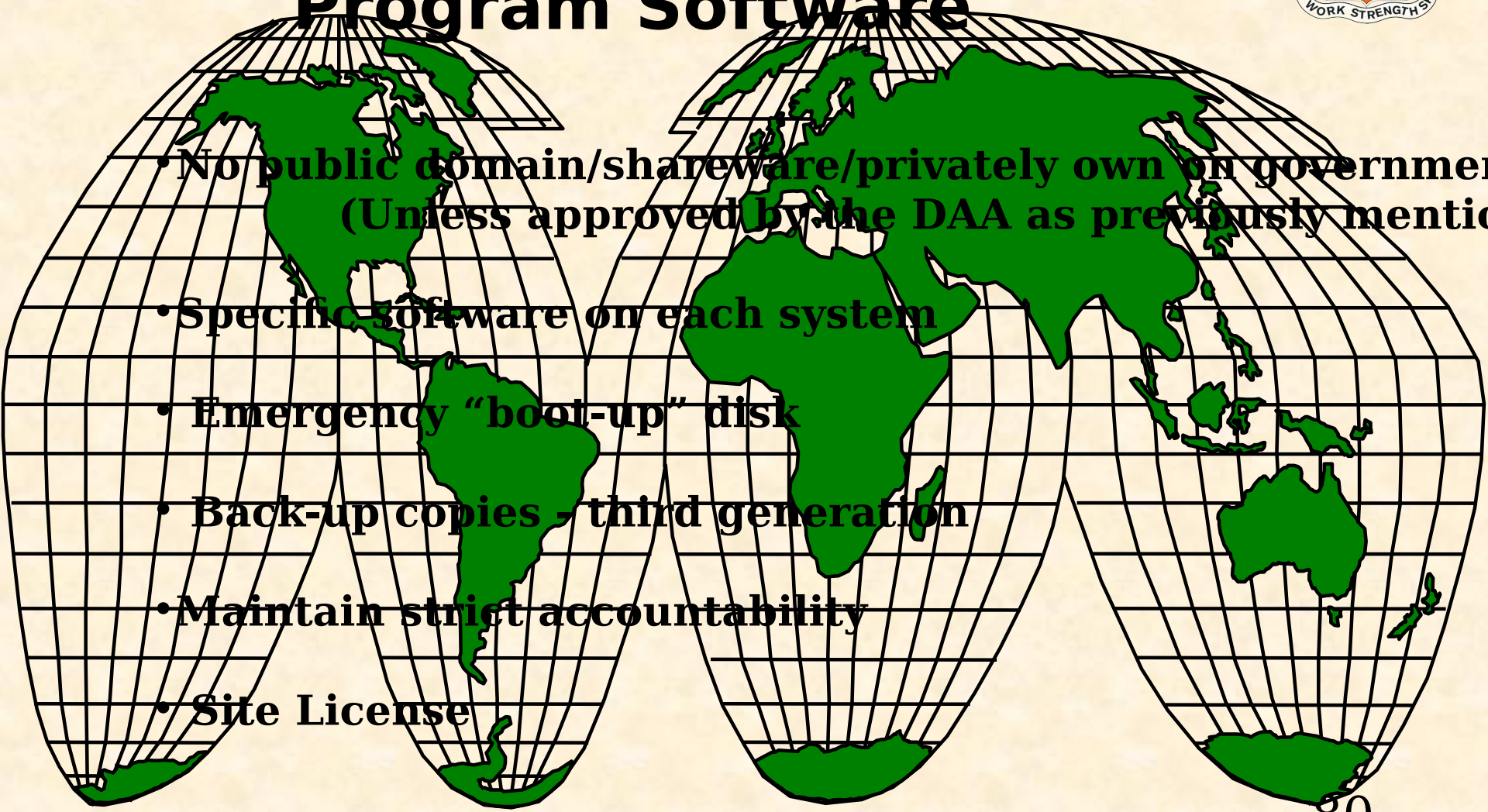
- **Environmental:**
  -- Do not eat or drink around computer system
  -- Ensure fire extinguisher is close by
  -- Use surge protectors

Automation Security Program Hardware



- High dollar value items
- Maintain strict accountability
- Do not interchange components without notifying the
- No privately own computer software in the work place

Automation Security Program Software



- No public domain/shareware/privately own on governme
  (Unless approved by the DAA as previously mentio
- Specific software on each system
- Emergency "boot-up" disk
- Back-up copies - third generation
- Maintain strict accountability
- Site License

Subversion and Espionage Directed Against the Army

AR 381-12

SAEDA Briefing

As a member of the U.S. Forces in Europe, you will have access to sensitive information, some classified. The U.S. Army Operations Security Program is designed to control and deny the enemy sensitive information. 43d Signal Battalion and the Intelligence Community needs your help in this effort.

▪index

What Types of Incidents Do You Report?

- Incidents of known, suspected, or possible espionage
- Suspicious questioning concerning military duties or required to provide military information
- Acts of deliberate compromise committed, attempted, or contemplated by DA personnel
- Contacts of DA personnel with known or suspected members of a foreign intelligence, military, or police agency
- Information concerning international terrorist activated or plans posing a direct threat to U.S. facilities or personnel

Who Do You Report SAEDA Incidents To?

- DA & HQ 5th Signal Command policy requires you to report SAEDA incidents directly to your local MI detachment
- Knowledge of a SAEDA incident will be limited to as few persons as possible and only those who have a need-to-know. Do not tell commander, co-workers, friends, spouses, etc.

SAEDA

Subversion and Espionage Directed Against the United States Army

- ***SUBVERSION:*** Attempt to undermine our faith in our country
- ***ESPIONAGE:*** Gather information that could injure Europe and t

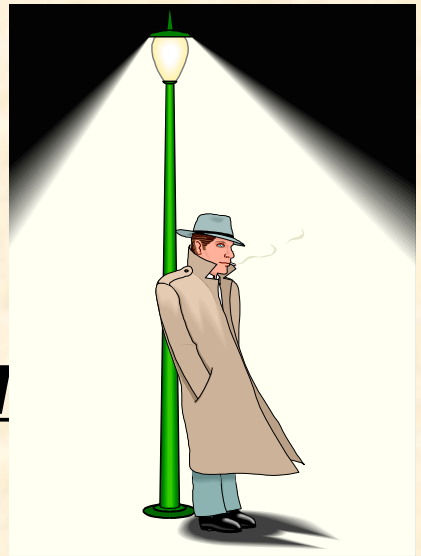
EACH OF US POSSES INFORMATION THAT IS VALUABLE TO THE S

- ***How are we approached?***

--Criminal or immoral conduct
--Indebtedness
--Illegal drugs

- ***What do we do when approached***

--Reported to your MI folks immediately



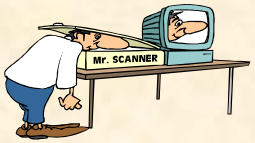
Spy Profile

- Usually Male
- Volunteers for espionage
- Motivated by greed
- Lives beyond means

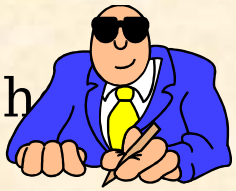
- Appears to be an outstanding soldier/employee (allows for more responsibility/greater access)
- AMORAL: Does not care for right/wrong

"Things to Avoid"

- Sexual seduction or misconduct



- Engaging in black market activities
- Accepting: Letters, photographs, packages, or other items to be smuggle out of country



- Signing of petitions/documents without ch with your country's Embassy/Consulate
- Photographing military facilities, soldiers, restricted/border areas, or anything of military signific t
- Talking to guides, interpreters, or other nationals wh appear too "friendly" and well informed of your job

SAEDA

Espionage Indicators

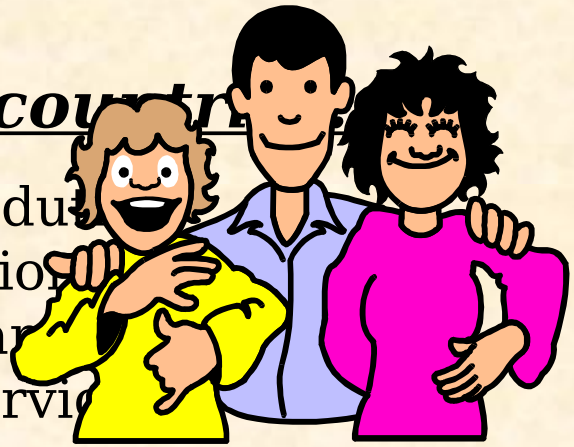
- Free spending (display of wealth)
- Sudden repayment of large debts
- Asking other to do unusual errands or favors for cash

- Unauthorized removal of classified documents
- Excessive use of duplicating machine
- Working excessive amounts of overtime when not required

- Frequent trips to “neutral” countries
- “Homesteading” in a position that is not one that people usually extend for (offers considerable access to sensitive information)

SAEDA

Incidents / Situations to Report



- ***Traveling to/through foreign countr***

--Subjected to questions regarding your du
--Requested to provide military informatio
--Threatened, Coerced, or pressured in a
cooperate with foreign intelligence servi

- Incidents of known, suspected, or possible espionage

- Other acts of deliberate compromised committed, at
or contemplated by personnel

43D Signal Battalion

SAEDA

“What to do after being approached”

- Neither flatly refuse nor agree to what is aske
- Remember details from the encounter
- Report incident immediately to the M.I.’s
- Do not attempt to investigate (James Bond method)

REPORT TO THE NEAREST MI OFFICE
In Mannheim
66th MI DET
Taylor Barracks
DSN 381-8276
After Duty Hours
DSN 380-1580

Report incident in person. Your report should be limited to those with a “NEED-TO-KNOW’

Operation Security - OPSEC

- AR 530-13
- Phone # (DSN) 370-8081/7848

▪index

Description

43d Signal Battalion Operations Security Program is designed to control and deny the enemy, sensitive information. All DA civilians and soldiers need to be briefed on their responsibilities in practicing good OPSEC.

The following OPSEC elements require your special attention:

Information Security 1

- Security to prevent disclosure of operation information by written, oral, or graphic communications
  - Protect, dispose of, and strip all maps as classified material, even strip maps or hand drawn maps of area
  - Use extreme caution when discussing field exercises, even with family members. Be careful with whom and where you discuss “going to the field”. The length and purpose of your absence and your field location could be critical information to the enemy

Signal Security -SIGSEC 2

- Security to prevent disclosure of information by telephone or radio
  - Do not discuss sensitive information over the telephone or an unsecured radio. Telephone and radio communications are monitored by unfriendly agents
  - Use secure voice telephone, AUTOSEVECOM, if available, for classified information. Classified electrically transmitted message channel should be used when secure voice is not available

▪index

Physical Security 3

- Security to prevent or limit hostile individuals access to military facilities, equipment, material, documents, and VIP personnel
  - Note that most of USAREUR military installations are protected by fences or walls and normally have gate guards assigned at entrances
  - Proper identification is required to enter USAREUR military installations and restricted areas within installations

Physical Security

- SF 702 Security Checklist
- Periodic Physical Security Inspections
- Safeguard door and computer keys (AR 190-51
- Notify handreceipt holder before releasing equ
- Confront unknown personnel in the work area

Physical Security (continued)

- Annual Security Briefings
- Additional equipment must be approved by the ISSO
- Report all compromises to ISSO Manager
- Don't eat or drink at computer terminal
- No authorized software
- Report all misuses to ISSO/ISSM
- Handle software correctly

Automation Security Program Physical Security Plan

- Key Control
- Security Activity Checklist
- COOP (Continuity of Operation Plan)
- Security Modes
- Passwords
- High Dollar value Items

You can prevent the enemy from gaining sensitive information when you practice good OPSEC. You are an important member of the 5th Signal Command OPSEC team and we are counting on you to do your part.

2d Signal Brigade Travel Policy

index

2d Signal Brigade Travel Policy

- The listings below will assist you in obtaining current travel advisory information via the internet:
  - http://www.state.gov
  - http://www.gsa.gov/travel.htm
  - http://travel.state.gov/travel_warnings.html

2d Signal Brigade Travel Policy

- You can also listen to travel warnings (as well as consular information sheets with facts about various countries and public announcements) 24 hours a day by calling stateside: 202-647-5225 from a touch tone phone.
- Printed information may be obtained by sending a self-addressed, stamped envelope to:
  - Office of Overseas Citizens Services
  - Room 4800, Department of State
  - Washington, DC 20520-4818
  - Write the name of the requested country or countries on the outside of the envelope

What are the Travel Warnings, Consular Information Sheets, & Public Announcements?

Travel Warnings

- Travel warnings are issued when the State Department decides, based on all relevant information, to recommend that Americans avoid travel to a certain country. Countries where avoidance of travel is recommended will have travel warnings as well as consular information sheets.

index

Public Announcements

- Public announcements are a means to disseminate information about terrorist threats and other relatively short-term and/or trans-national conditions posing significant risks to the security of American travelers. They are made any time there is a perceived threat and usually have Americans as a particular target group. In the past, public announcements have been issued to deal with short-term coups, bomb threats to airlines, violence by terrorists, and anniversary dates of specific terrorist events.

index

Consular Information Sheets

- Consular information sheets are available for every country in the world. They include such information as location of the U.S. Embassy or Consulate in the subject country, unusual immigration practices, health conditions, minor political disturbances, unusual currency and entry regulations, crime and security information, and drug penalties. If an unstable condition exists in a country that is not severe enough to warrant a travel warning, a description of the condition(s) may be included under an optional section entitled “areas of instability.” On limited occasions, also restated in this section, any U.S. Embassy advice given to official employees. Consular information sheets generally do not include advice, but present information in a factual manner in order for the traveler to make his or her own decision concerning travel to a particular country.

index

Reporting Foreign Travel

- IAW DoD 5105.21-M-1, August 1998: All personnel who plan official or unofficial travel (outside country of residence) will report travel plans to their supervisor to complete required documentation.

index

Travel

Remember…….

- You are a prime target for FIS Agents
- Smuggling, black marketing, illegal currency dealings
- Moral indiscretion, accepting packages
- Do not sign petitions
- Do not take photos of Military Installations
- Be suspicious of very friendly persons
- Don’t falsify a VISA (asks home address, profession, e
- If you are being followed, don’t play games
- Telephones are tapped
- Baggage will be search
- Two-way mirrors
- Look at human weakness, if none, they will
- Report anything suspicious immediately

Foreign National Access to Installations in USAREUR

- AR 380-67 20 Jan 88, USAREUR Suppl 1 (Page 22, para 3-707)
- Updated list of countries, Memo, 01 Apr 99
  - » The specified country passport holders are not allowed on USAREUR installations where access is controlled. (This means that they are NOT allowed on post)
  - » Any attempts by these personnel to gain entry to the installation must be reported to Military Police and Military Intelligence immediately.

▪index

Specified Country List

Albania Afghanistan Angola
Bulgaria Burma Cambodia China
Cuba Estonia Ethiopia
Georgia Iran Iraq Laos
Latvia Lebanon Libya
Lithuania Outer Mongolia Nicaragua North
Korea Peru Romania South
Africa Syria Tibet Vietnam
Yemen

All portions of the former USSR.

Former Yugoslavia (Serbia, Montenegro, and
Bosnia Herzegovina)

Staff Assistance Visit (SAV)

index

Staff Assistance Visits (SAV)

- Staff Assistance Visits (SAVs) will be conducted once a year or upon request. The SAV will be conducted by the security personnel to instruct personnel and identify security program deficiencies.

Privately Owed Firearms (USAREUR Reg 190-6)

- Ownership of a firearm in USAREUR is not a right, it's a privilege!
- Ensure all weapons are registered with the Provost Marshal and the Bundesverwaltungsamt
- Brief family members on handling firearms
- Store firearms unloaded in a locked container with ammo stored separately.
- Military E-4 and below, unmarried, unaccompanied, living on post must keep firearms in the arms room

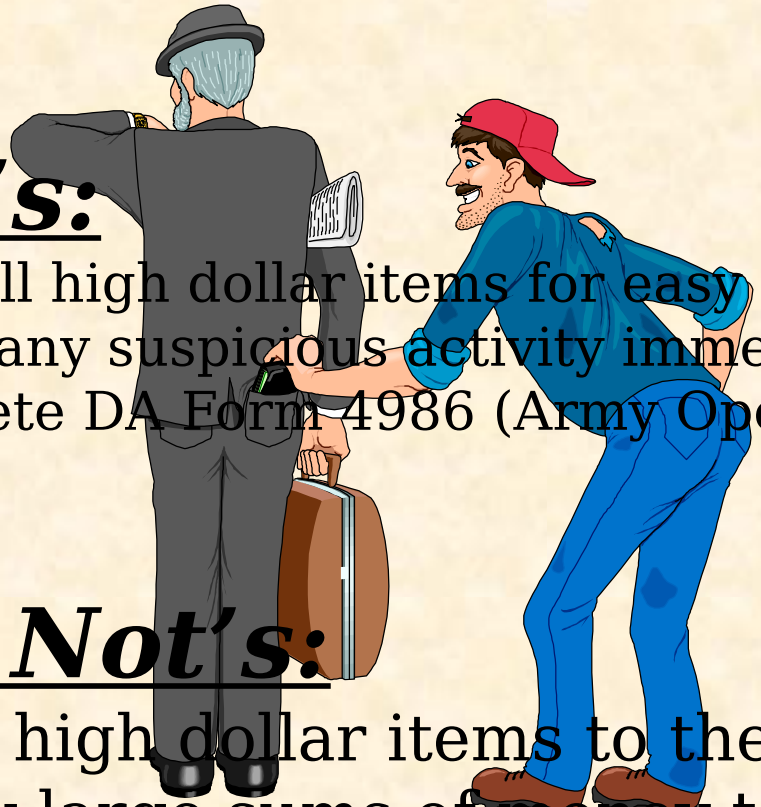
- **Carrying a firearm:**

  -- Possession of 190-6B
  -- Unloaded and wrapped
  -- Do not conceal on person

Click here forWeapons Update!

▪index

Crime Prevention



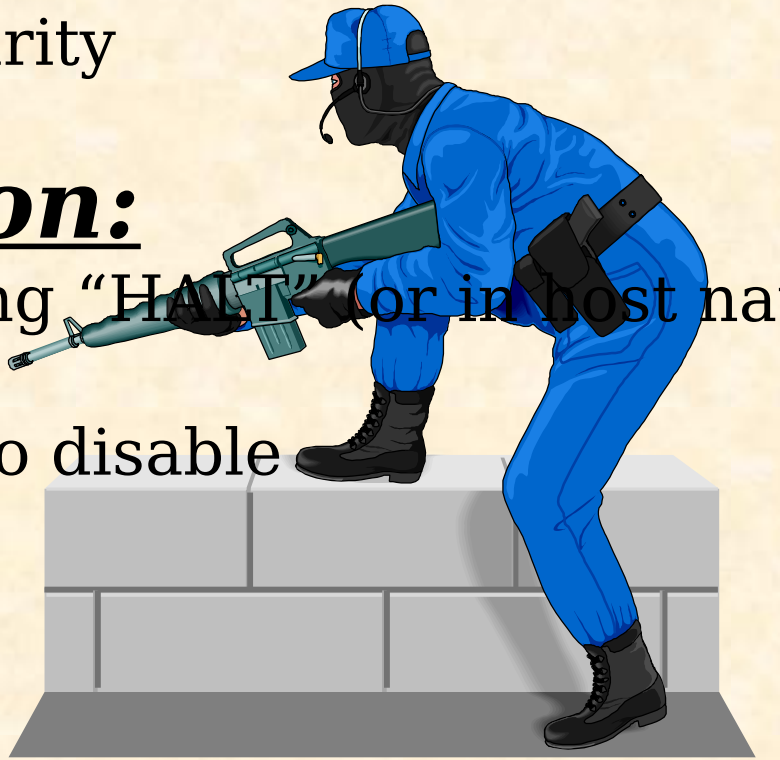
- ***Do's:***
- Mark all high dollar items for easy identification
- report any suspicious activity immediately
- Complete DA Form 4986 (Army Operation Identification)

- ***Do Not's:***
- Bring high dollar items to the work place
- Carry large sums of money to the work place
- Leave your purse (bag) unattended for a short

Use of Force

- ***Minimum force necessary:***
  -- Protect a person's life
  -- Protect National Security

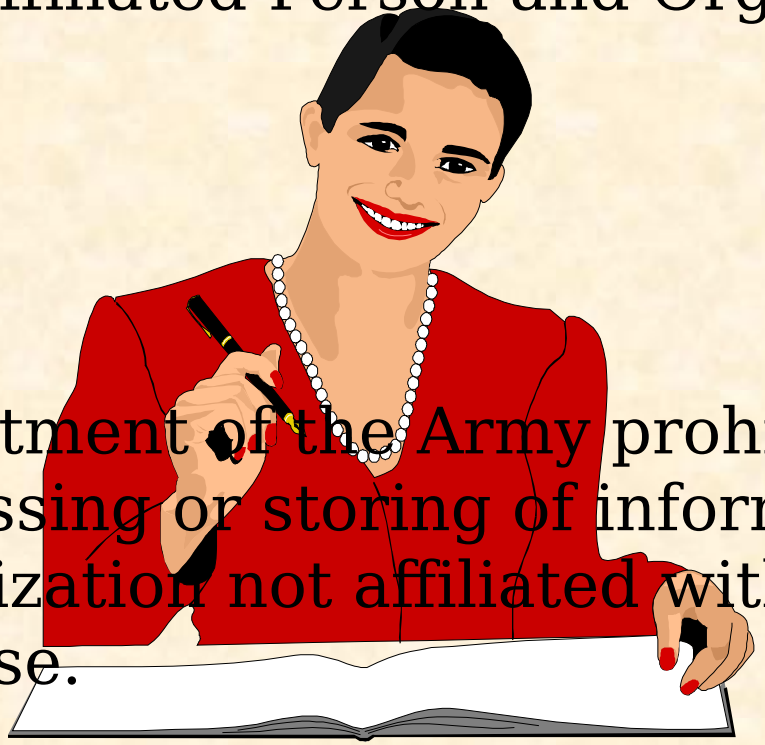
- ***Firing a weapon:***
  -- Only after commanding "HALT" (or in host nation
  -- No "Warning Shots"
  -- Shots will be aimed to disable



- ***Deadly force:***
  -- Verbal persuasions
  -- Self defense

Non-Affiliated Persons

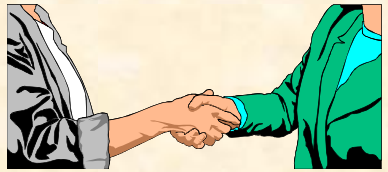
Acquisition & Storage of Information concernin
Non-affiliated Person and Organizations



Department of the Army prohibits acquiring, re
processing or storing of information on person
organization not affiliated with the Department
Defense.

Standards of Conduct

- **Conflict of Interest:**
  -- Knowledge of technical information passed on for special favors or money
- ***Gratuities:***
  -- Will not be accepted
- ***Gifts:***
  -- No person will donate more than $10.00 for the purchase of any gift.



Outside employment:
-- Will not use government resources in connection with an outside business

Use of Government facilities:
-- Strictly for Government Use Only

Links/Regulations/Phone Numbers

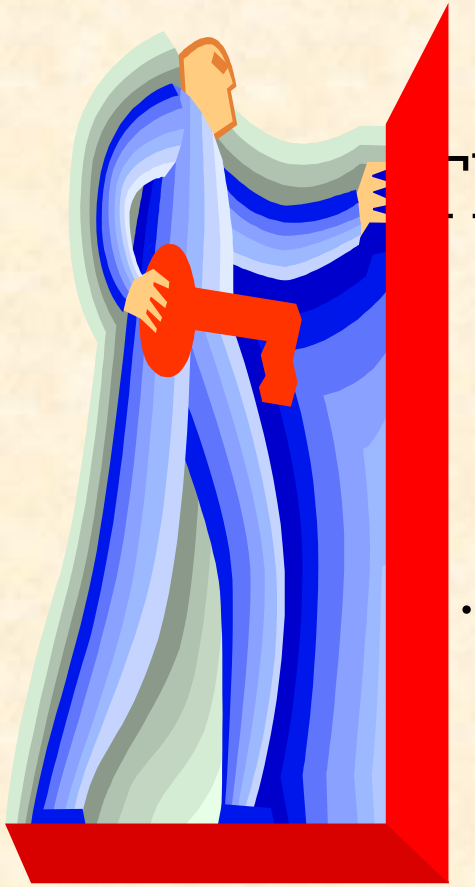
- **AR 380-5**, 25 Feb 88 and all subsequent changes, Classification Management
- **AR 380-19**, Information System
- **AR 380-53**, Information System Security Monitoring Security
- **AR 380-67**, Personnel Security
- **AR 380-67** and UR Supp 1, Foreign National Access
- **AR 381-12**, SAEDA
- **AR 530-13,** OPSEC
- **UR 190-6**, Privately Owned Firearms
- **DoD Reg 5105.21-M-1**, Reporting Foreign Travel

index

Links/Regulations/Phone Numbers (continued)

- Travel Advisories can be found at the following web sites:
  - -http://www.state.gov
  - -http://www.gsa.gov/travel.htm
  - -http://travel.state.gov/travel_warnings.html
- Regulations and Forms can be found at the following web sites:
  - -Army Electronic Publications & Forms - Department of the Army
  - -Library of AE Publications & Forms - Main Menu
  - -Forms Program Home Page
  - -NISPOM.COM
- Your local Security Advisor/Manager can be contacted by calling 37
- Or you can Email us.

END OF BRIEFING



This concludes this briefing

Thank You…

…To receive credit, please click ON THIS L

(Subject line: “Annual Briefing”)

(Body of Message: Name, rank, unit and section